RSAC 2025 Conference

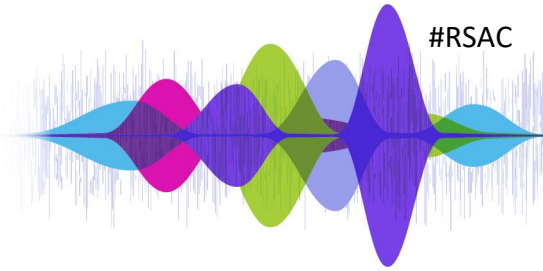
Many Voices.
One Community.

SESSION ID: TPV-W09

Got Supply Pain: A Real-World Approach to Supply Chain SDL

Richard Tonry
Distinguished Engineer
Firmware Security Architect
Dell

Mohit Arora
Senior Distinguished Engineer
Software Security Architect
Dell



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC™ 2025 Conference

Rhetorical Question

RSAC™ 2025 Conference

Where's the supplier's threat model?

Engineers…

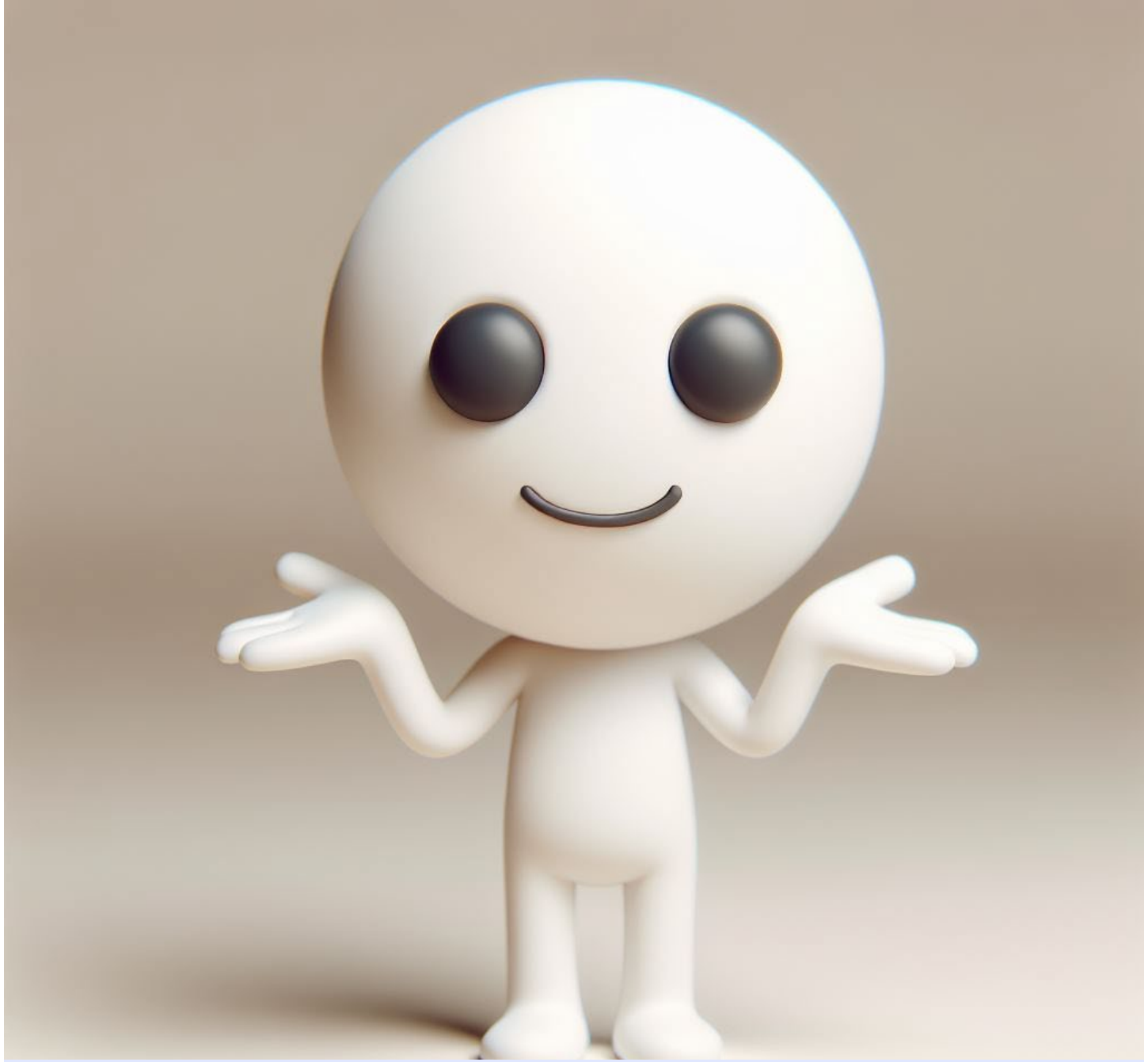
¯_(ツ)_/¯

RSAC™ 2025 Conference

How many of you have asked your suppliers for their threat model?

Many Voices.
One Community.

Supplier…



AI Prompt: Use the ascii art to generate a generative AI version of this ASCII art. ¯_(ツ)_/¯

RSAC™ 2025 Conference

How many of you have asked your suppliers for their pen-testing?

Many Voices.
One Community.

Supplier…

AI Prompt: Make it a 3-D cartoon

RSAC™ 2025 Conference

How many of you have asked your suppliers for their SDL artifacts?

Many Voices.
One Community.

Supplier…

AI Prompt: Add more gestures and expressions.

RSAC™ 2025 Conference

How many of you have asked your suppliers for their SDL process?

Many Voices.
One Community.

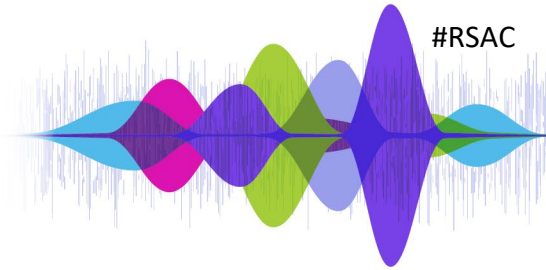
Supplier…

AI Prompt: Make the character a person with a confused and exaggerated expression,. eyes rolling

Lawyers…

AI Prompt: “Create a scene of lawyers sitting around a conference table with one side looking confused and the other side looking worried”

Objectives



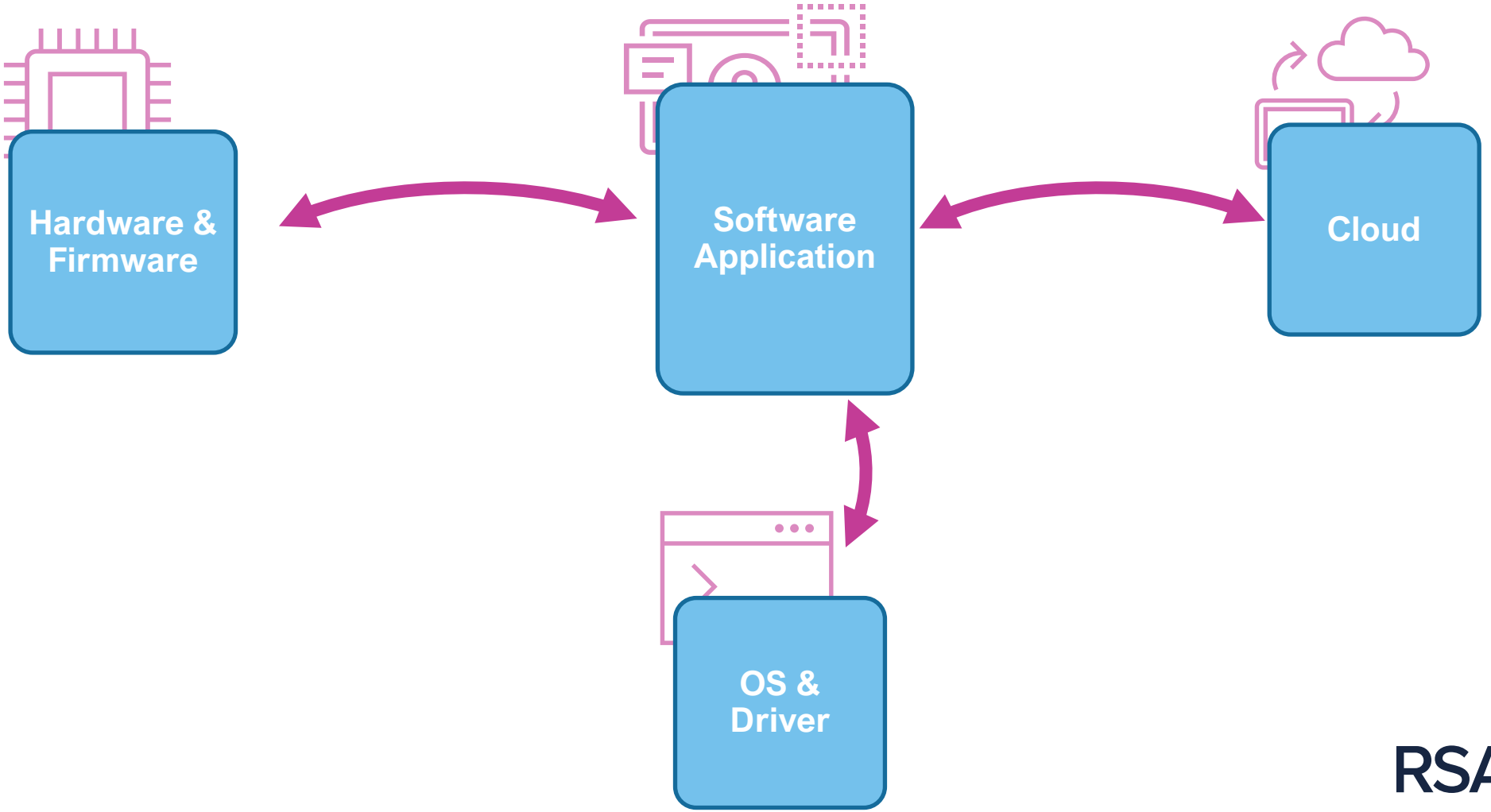
- Expanding Secure Development Lifecycle (SDL) to suppliers
- Operationalizing and industry collaboration
- Key takeaways and next steps

One SDL to Rule the World

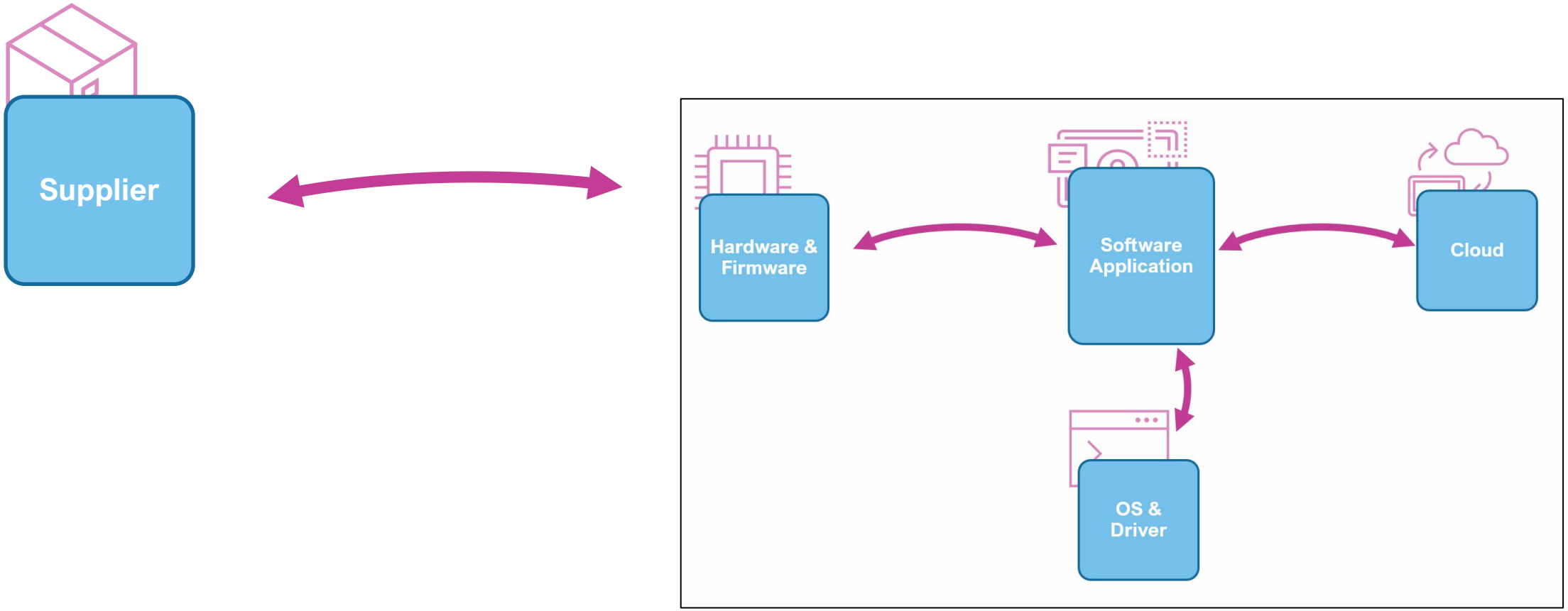
- Extension of our previous talk on scaling SDL across the technology stack
- Full stack SDL across Hardware, Firmware, Software, Cloud

https://www.rsaconference.com/library/presentation/electrons-to-cloudsone-sdl-to-rule-the-world-from-hardware-to-the-cloud

Full Stack SDL



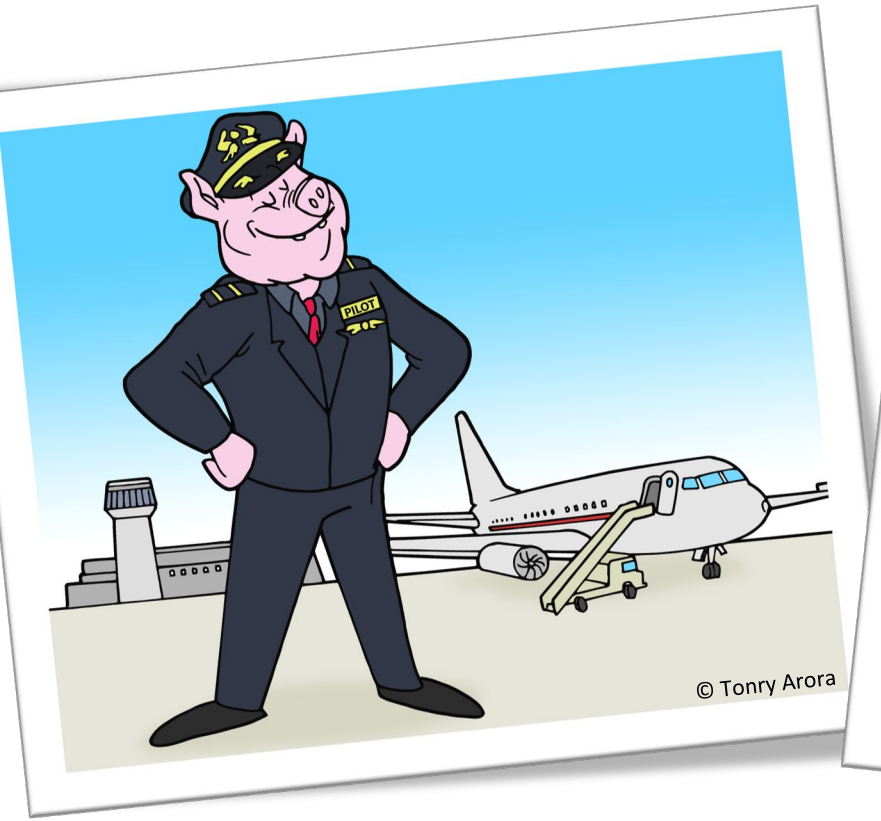
Full Stack Supply Chain SDL

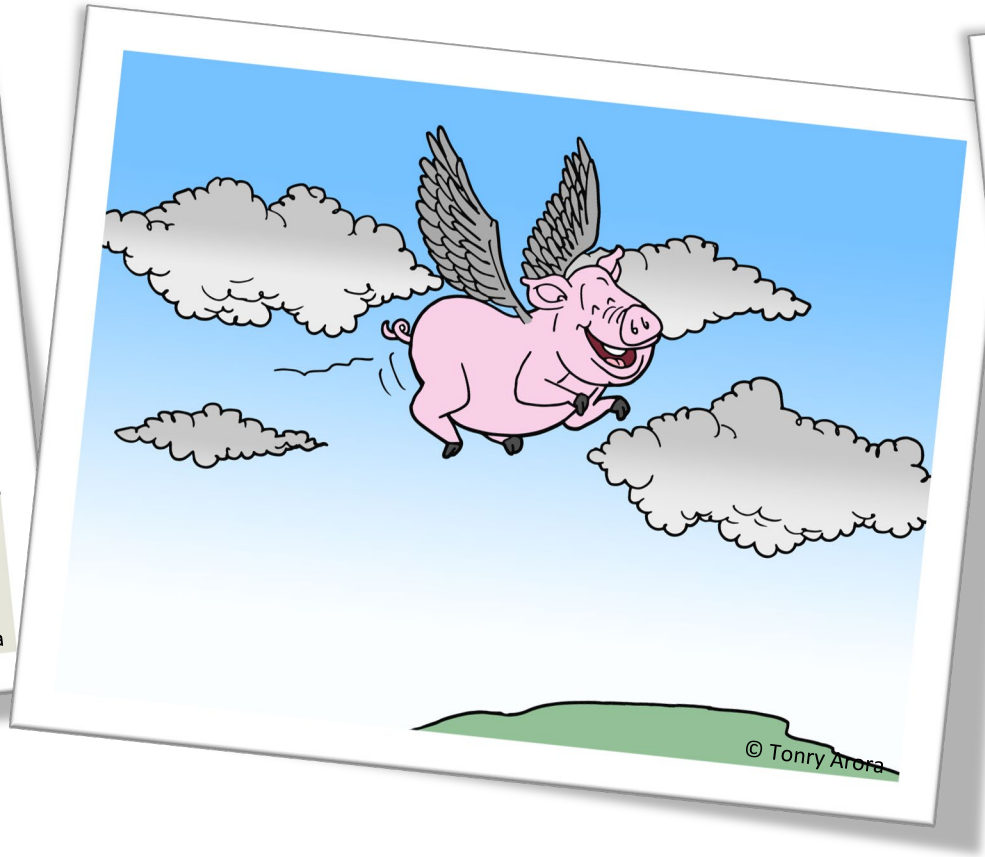


Where's your Threat Model?

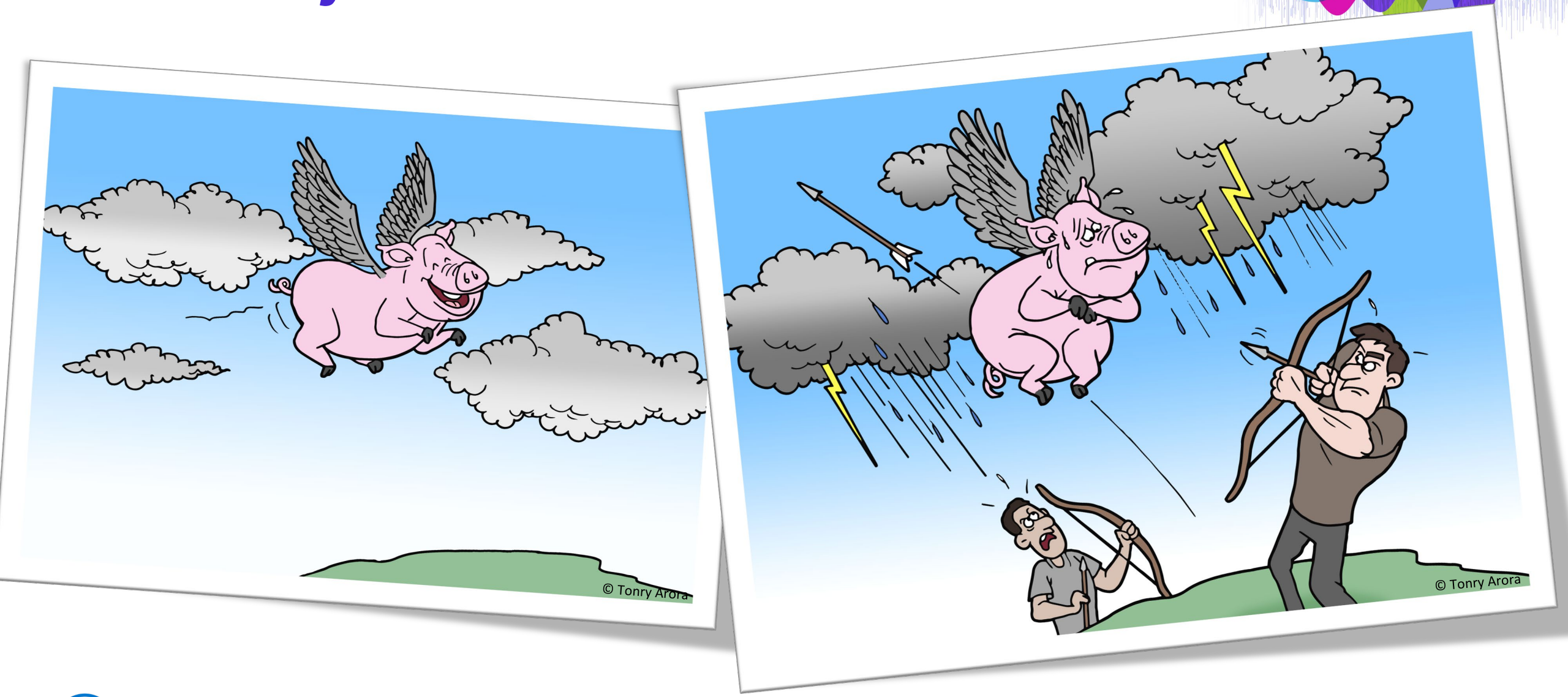
Threat Model Example
Pigs Flying

Where's your Threat Model?



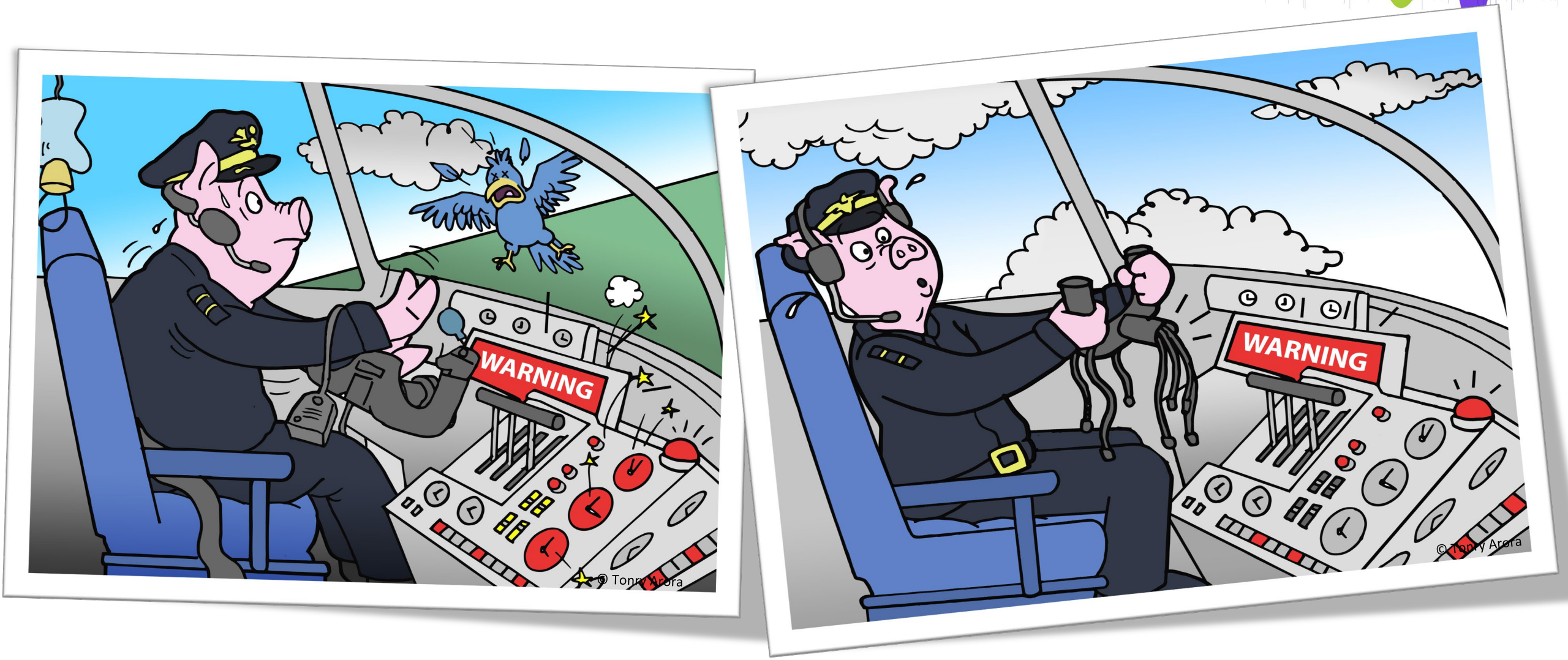


Where's your Threat Model?

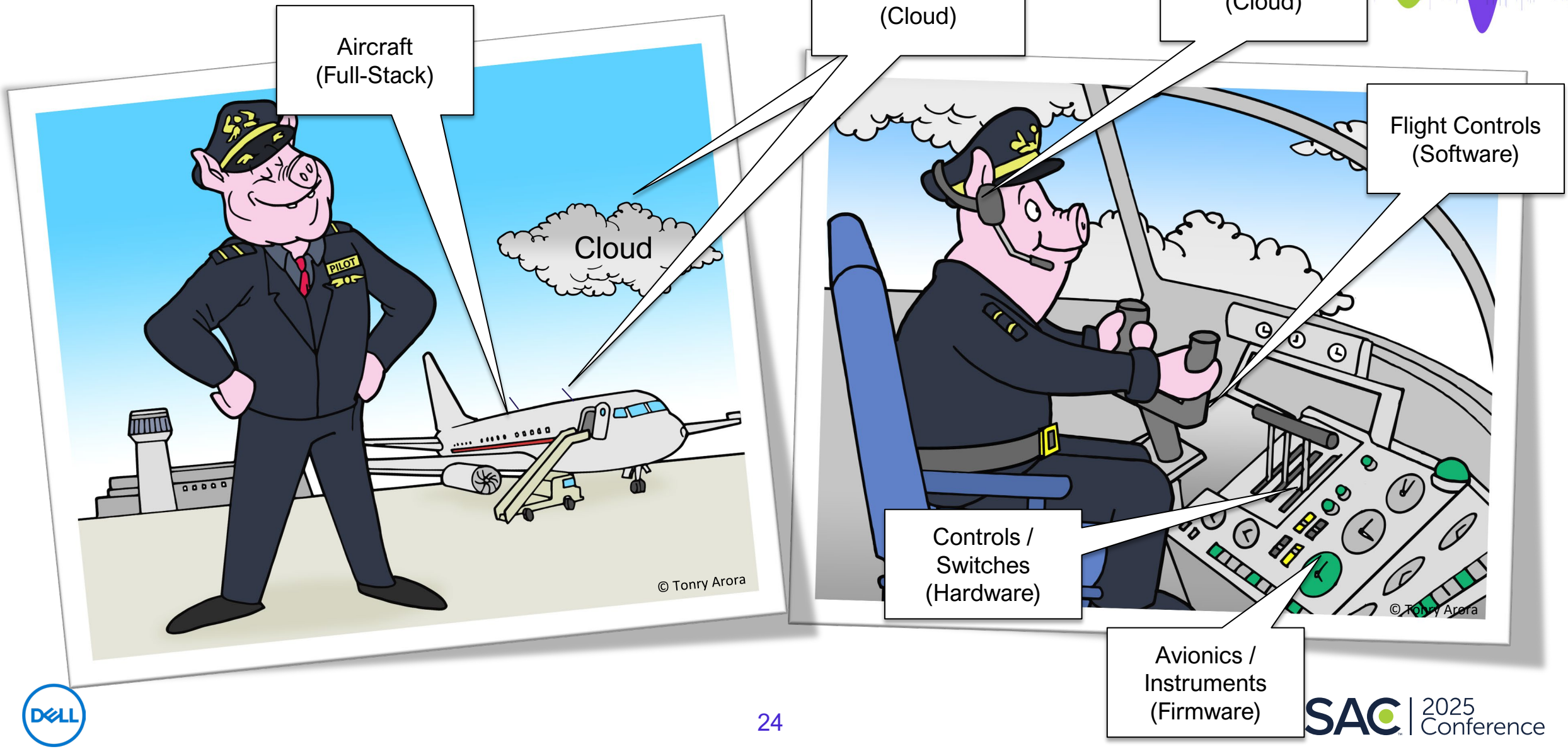


Where's your Threat Model?

Where's your Threat Model?



Where's your Threat Model?



RSAC 2025 Conference

Got SDL?

Our Approach for One SDL

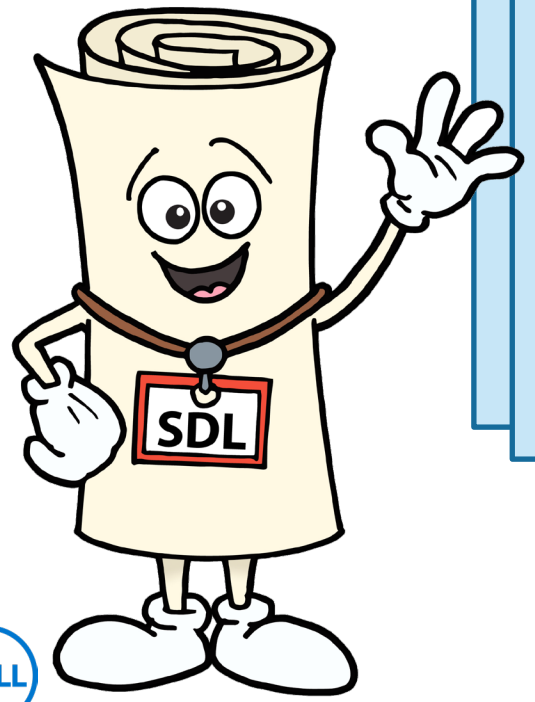
SDL Policy

SDL Controls

- Design
- Verification
- Data protection
- Web security
- Injection prevention
- 3rd Party Component
- Documentation
- Governance

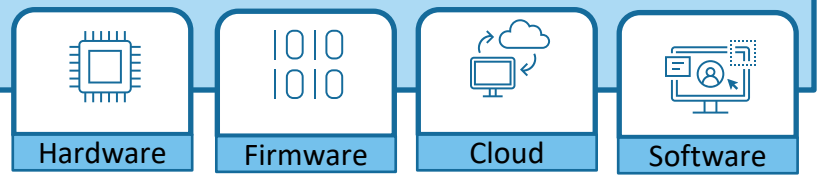
Control

- Objective
- Scope
- Applicability
- Requirements
- Guidance
- Verification

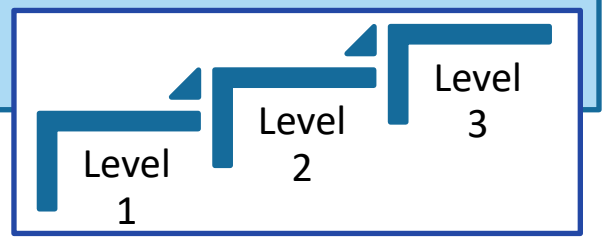


Our Approach for One SDL

Each control provides technology stack specific applicability, requirements, guidance and verification activities

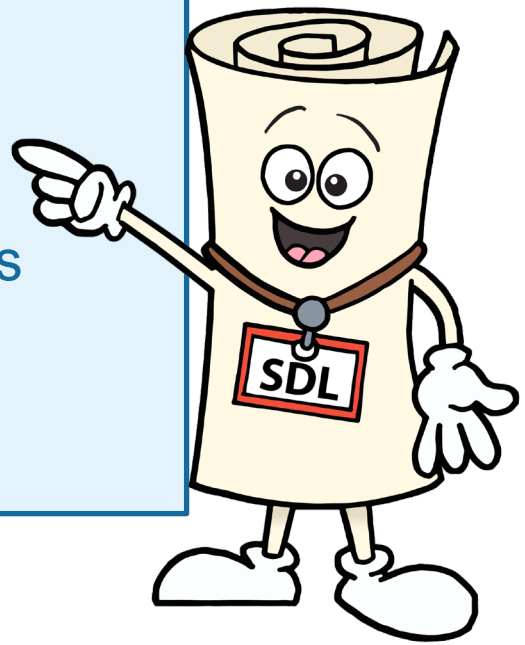


Each control also provides requirements and verification activities based on SDL maturity levels



Control

- Objective
- Scope
- Applicability
- Requirements
- Guidance
- Verification

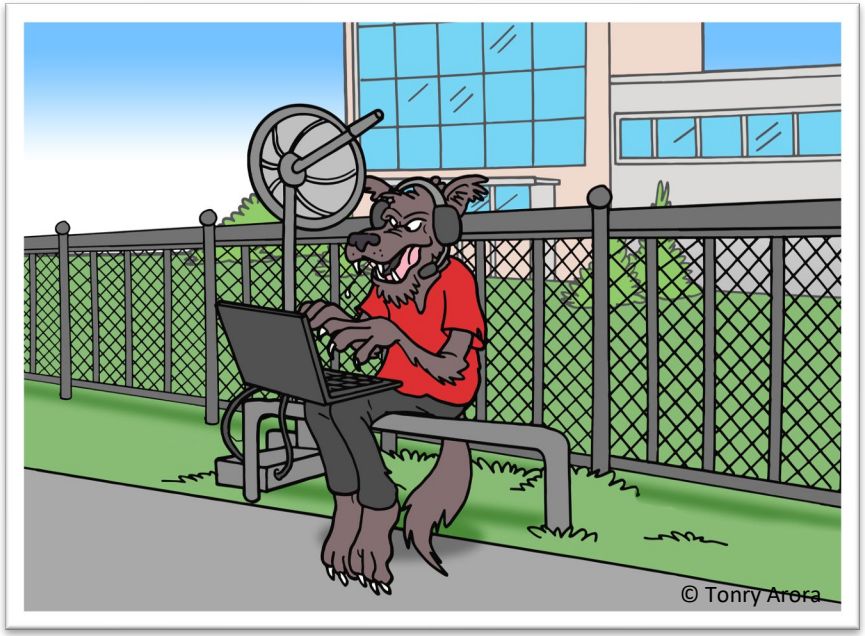


RSAC 2025 Conference

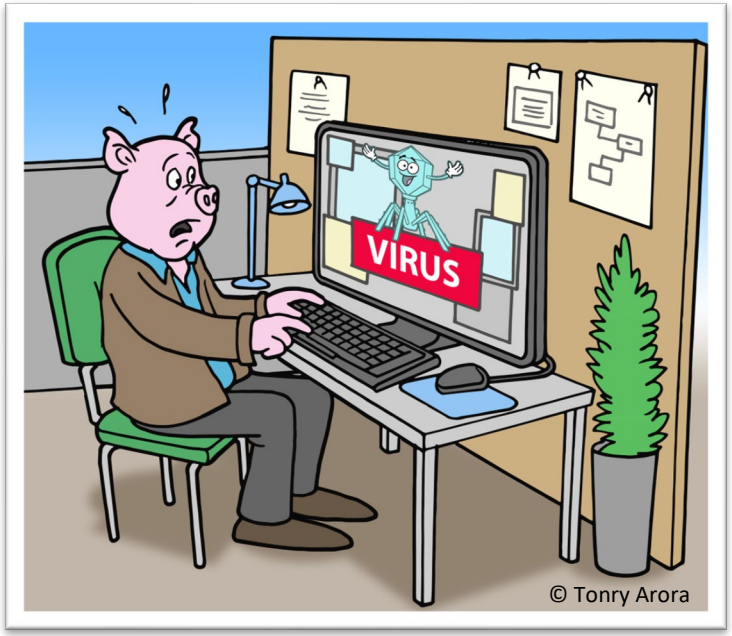
Expanding SDL to Suppliers

Beyond Supply Chain SDL

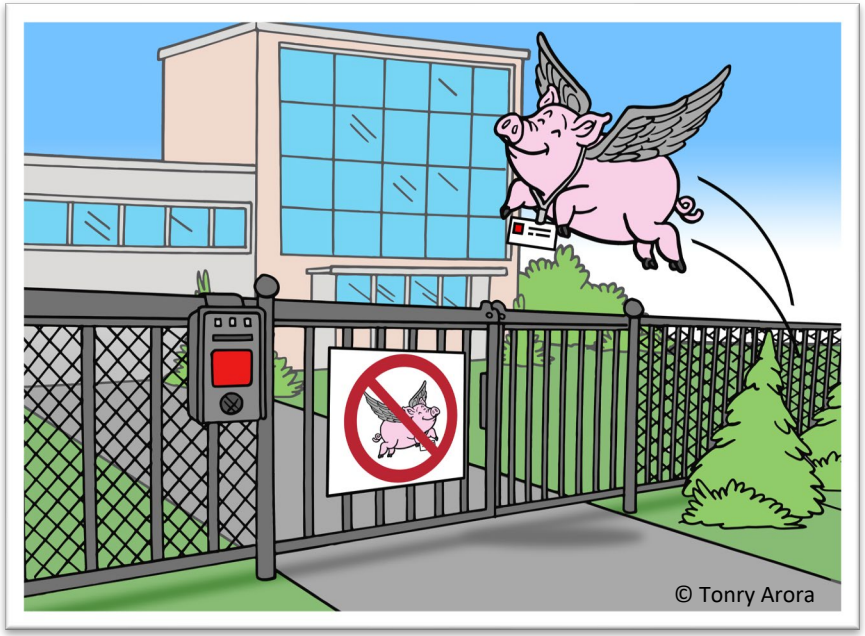
Infrastructure Security



Information Security

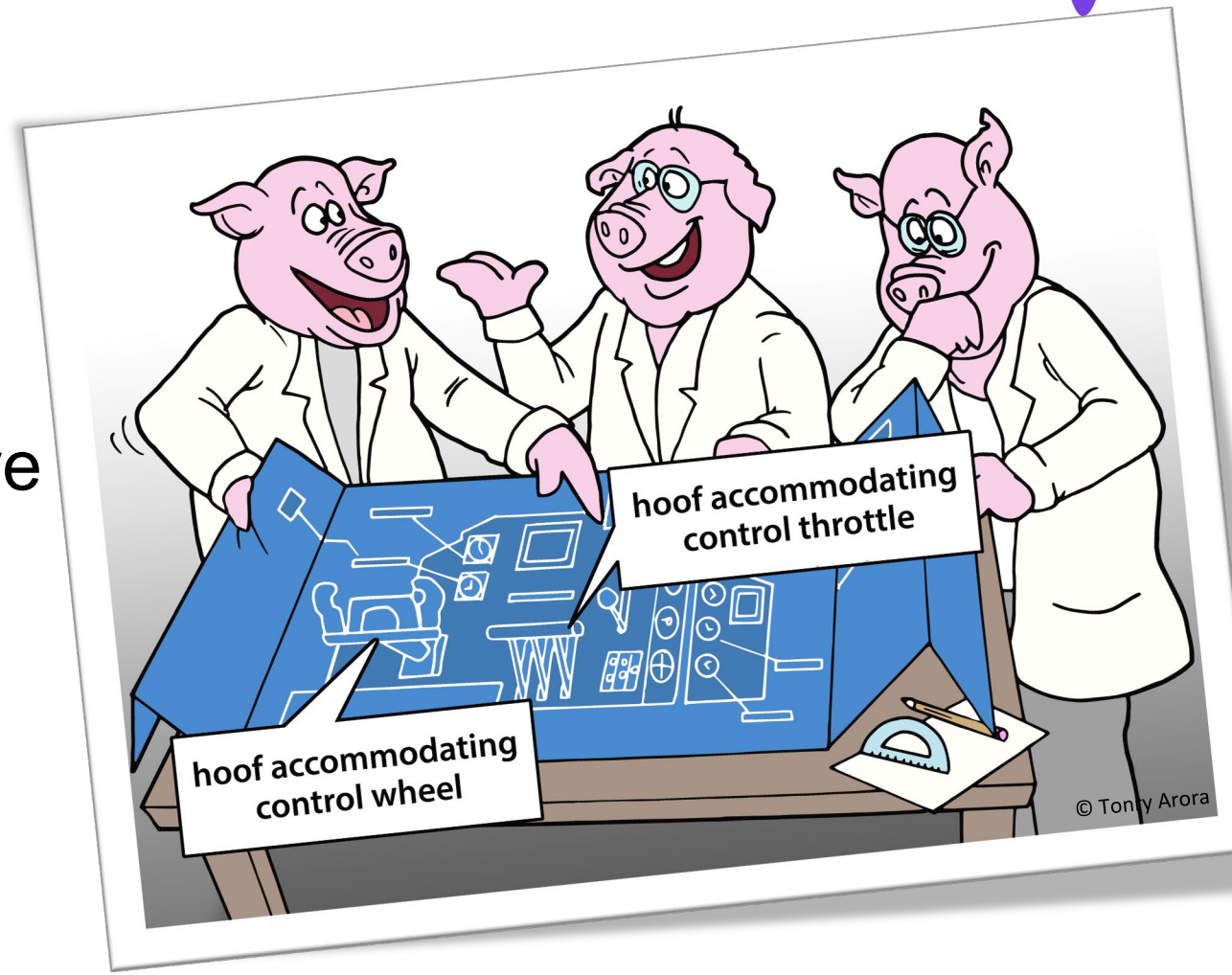


Physical Security



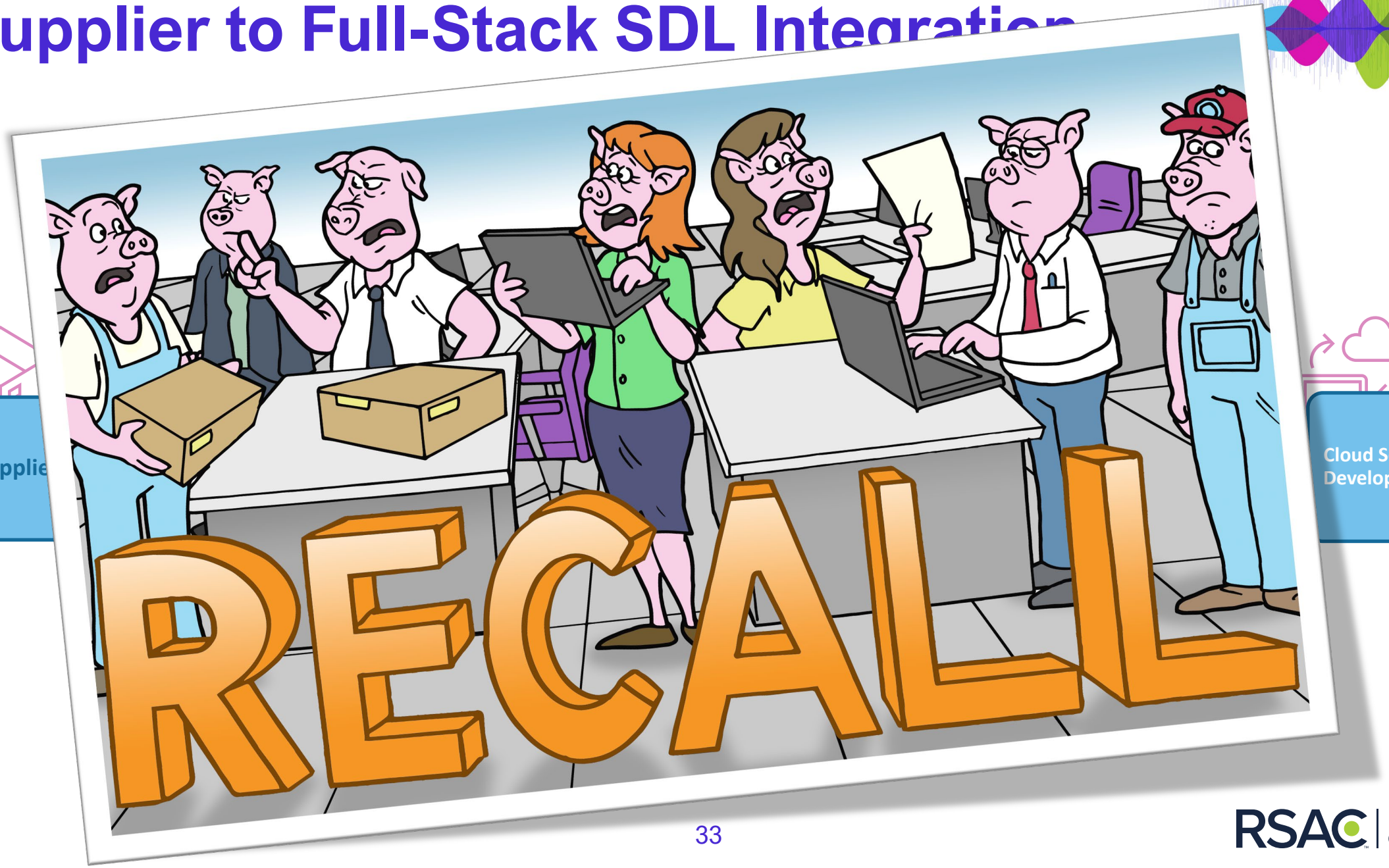
Expand SDL to Suppliers

- Supplier SDL to Full-Stack SDL integration
- From the engineering perspective
- SDL starts with the supplier



Supplier to Full-Stack SDL Integration

Supplier to Full-Stack SDL Integration

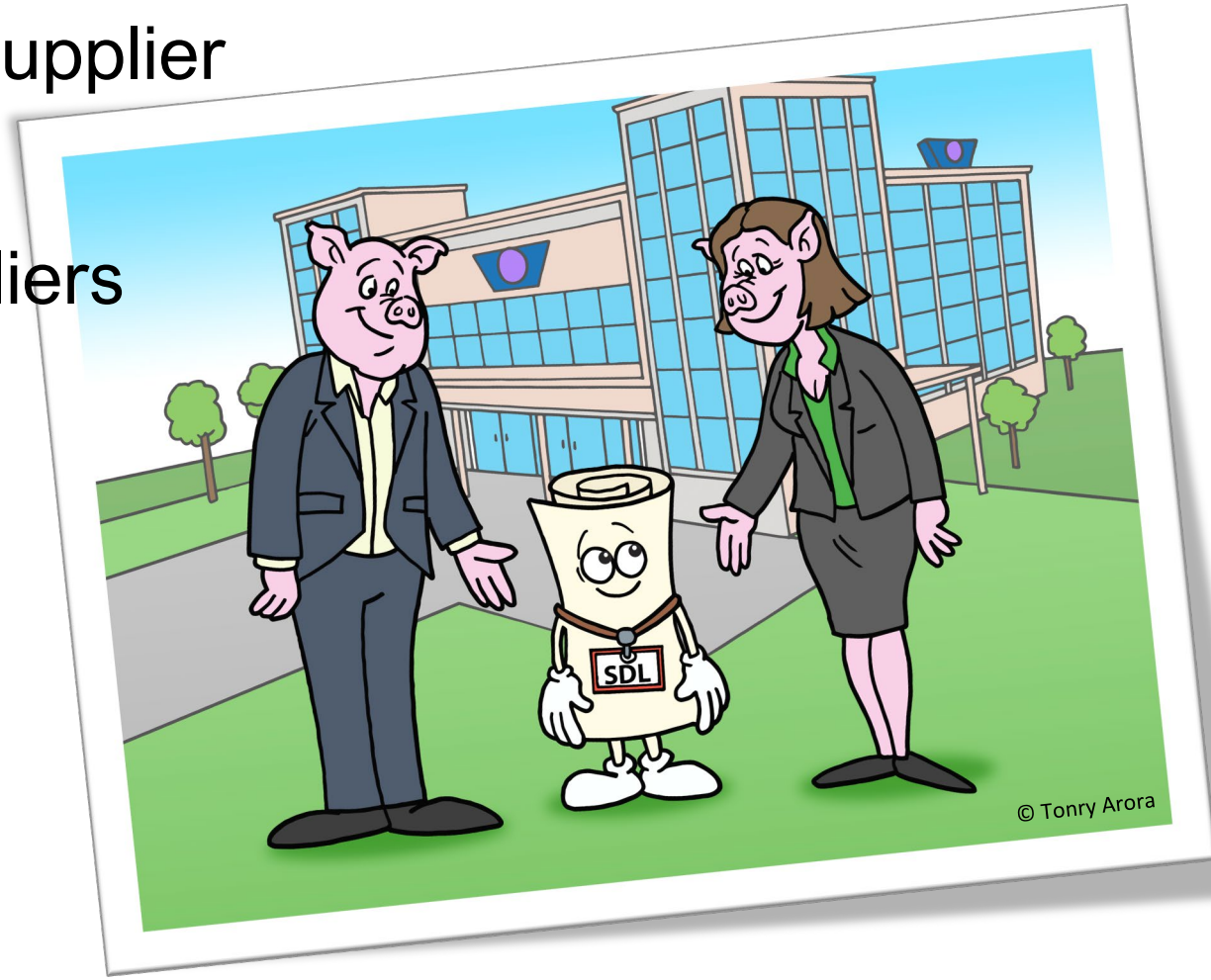


Supplie

Cloud Service Development

Supply Chain SDL End-to-End View

- Expand SDL requirements to the supplier components
- Full-stack SDL includes your suppliers
- Follow your organization security standards
- Supplier's SDL attestations



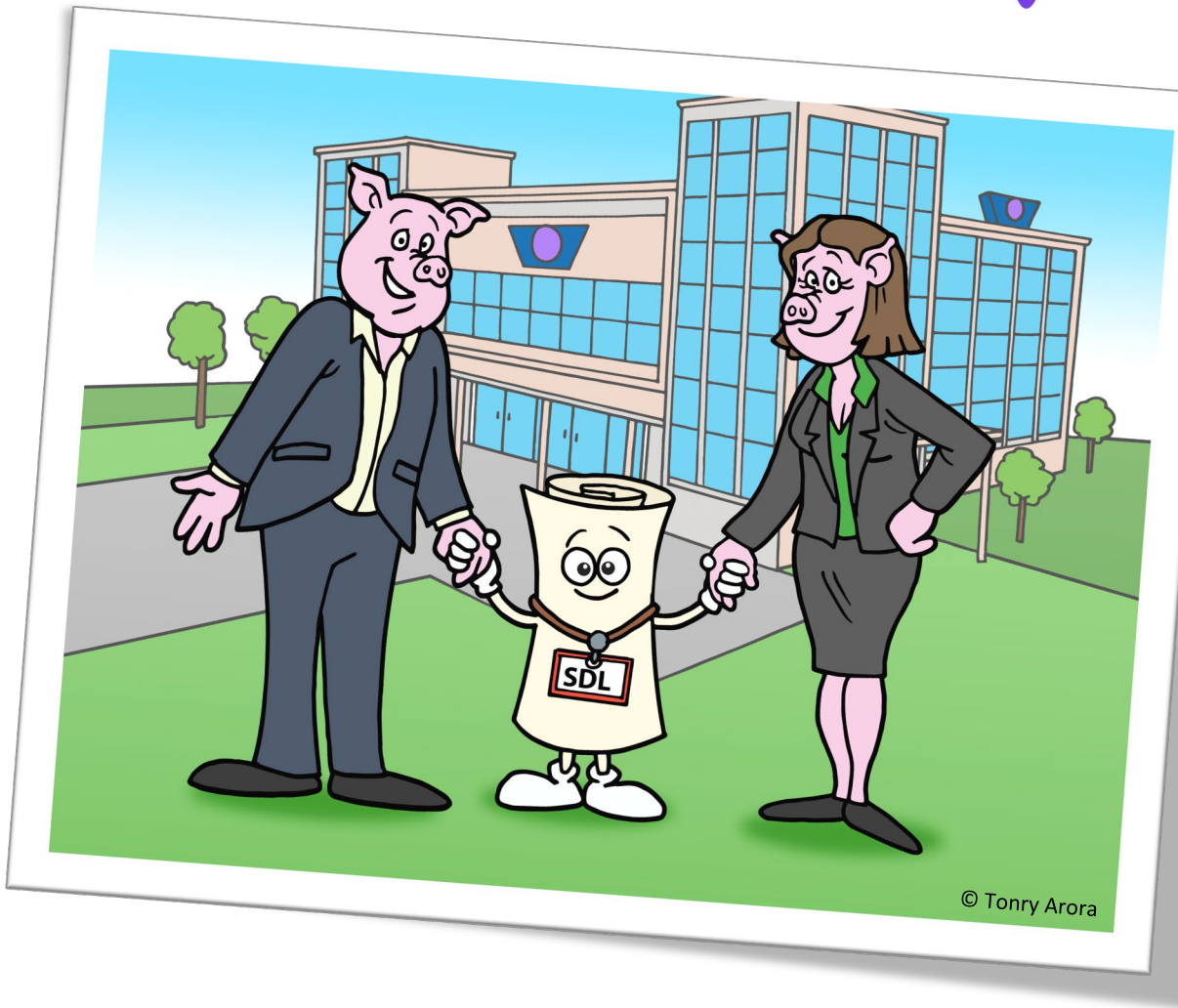
Supply Cl

- Expand SD
  component
- Full-stack S
- Follow you
  standards
- Supplier's

AI Prompt: Make the character a person with a confused and exaggerated expression,. eyes rolling

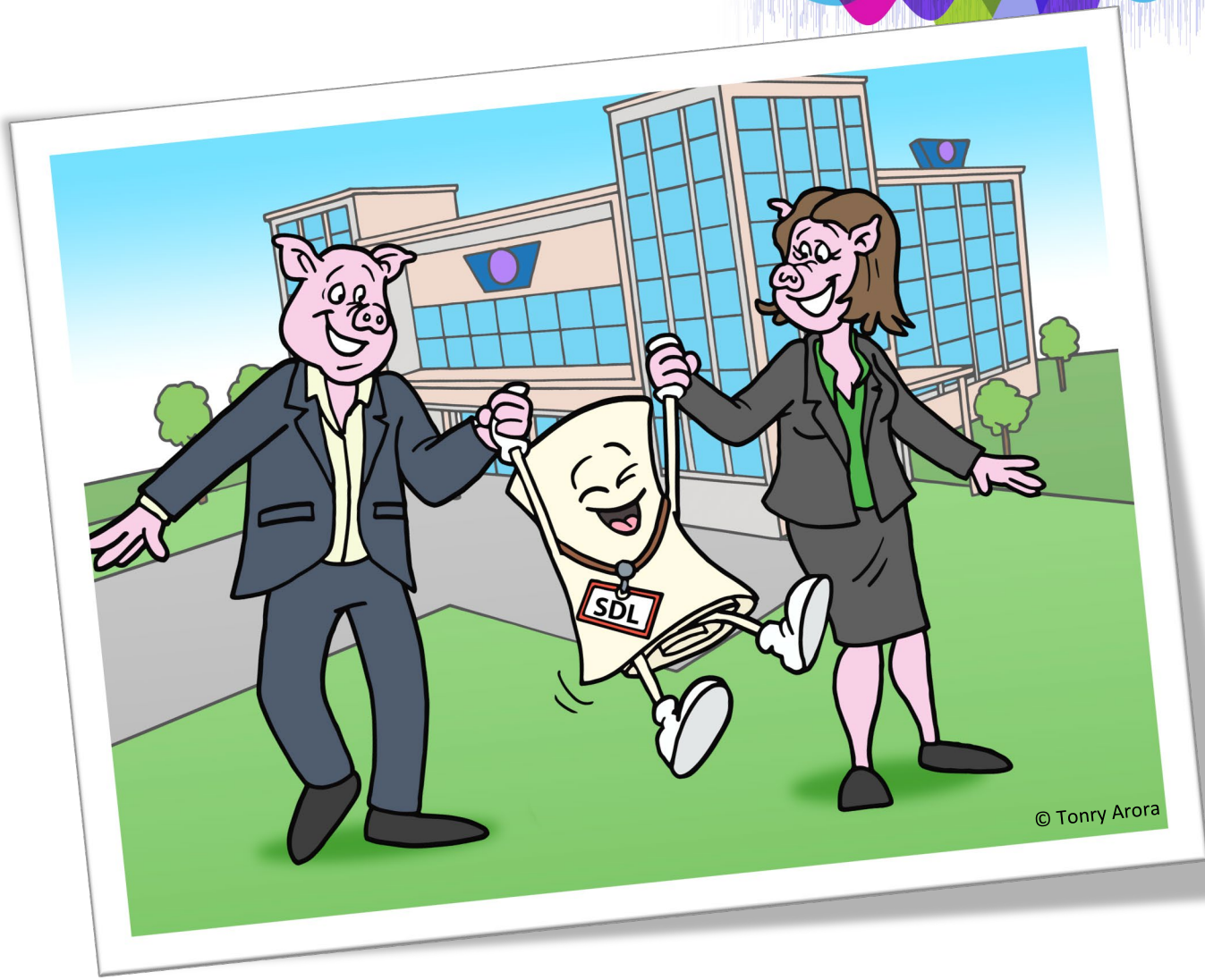
Add Supplier SDL Requirements

- Mapping requirements
- Supplier scale and complexity
- Product scale and complexity
- Complexity across the technology stack



Shifting SDL Left(er)

- SDL beyond attestation
- Align on industry standards
- Why go beyond attestation?
- Mitigate the Fear!



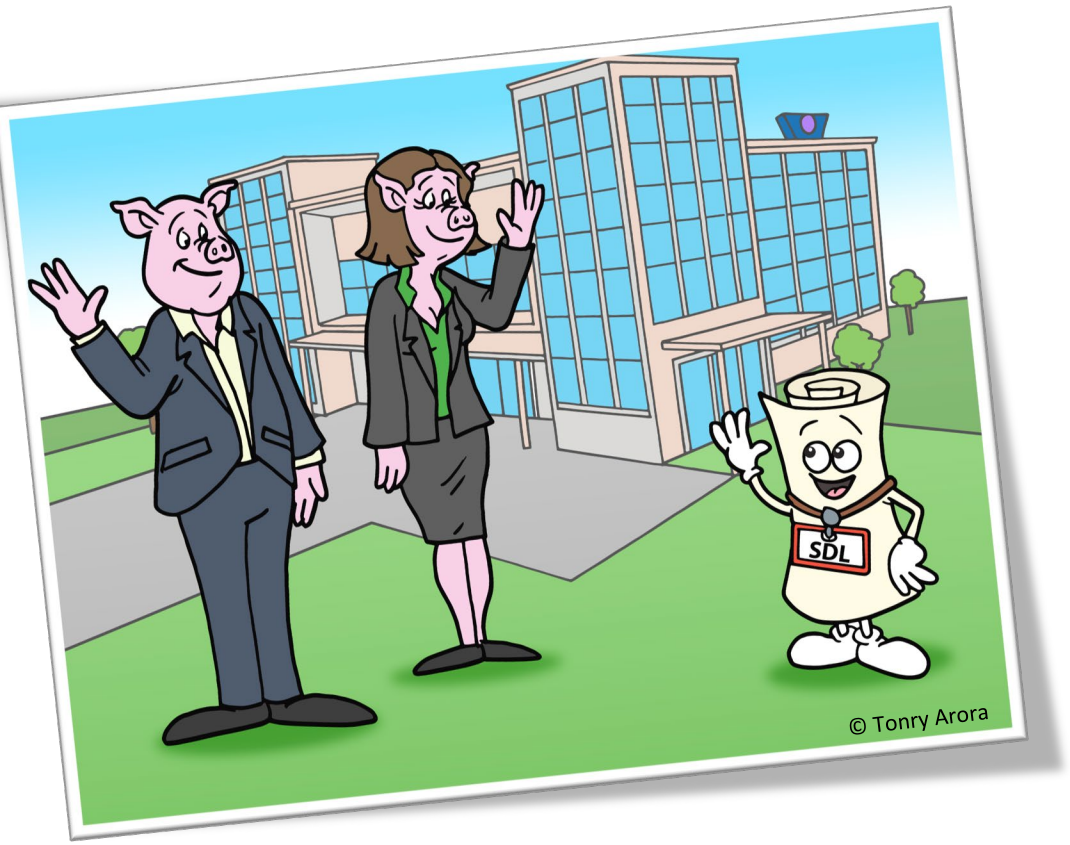
RSAC 2025 Conference

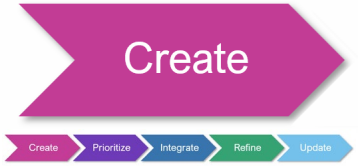
Operationalizing Supply Chain SDL

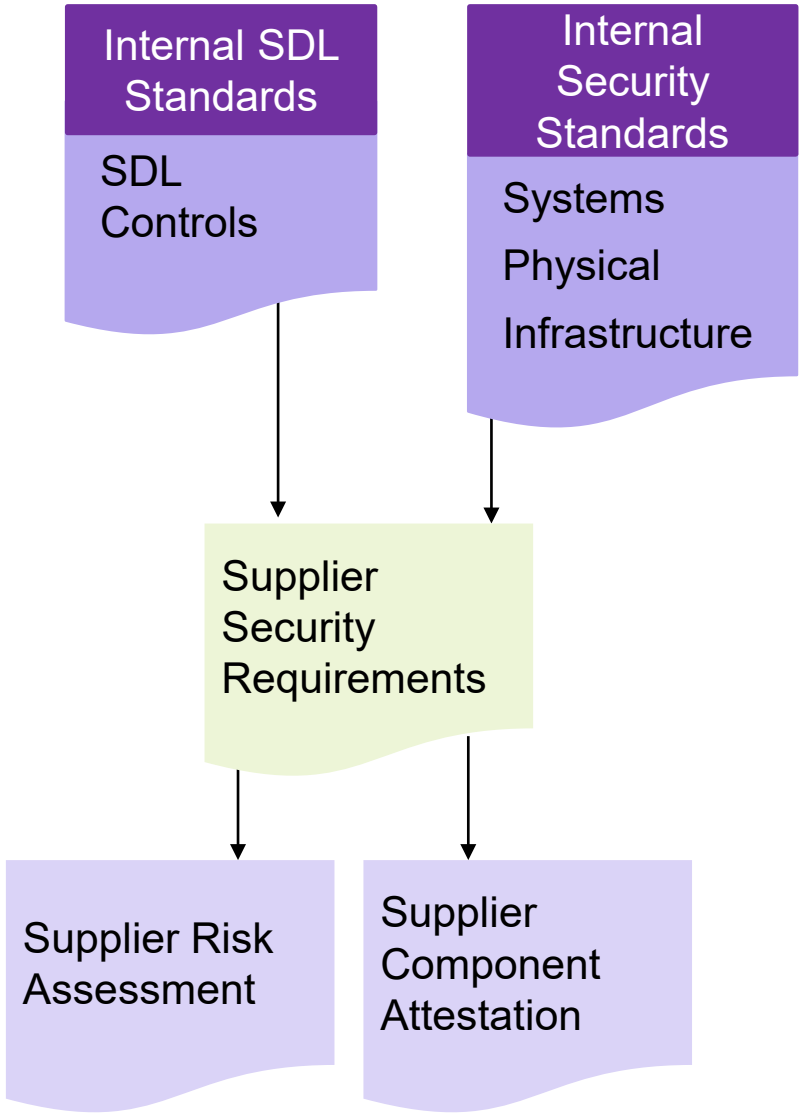
Overall Process View

Create	Prioritize	Integrate	Refine	Update
Define supplier standards and assessments	Prioritize starting with critical suppliers	Integration across development processes	Solicit feedback to refine the process	Update process and extend to next set of suppliers

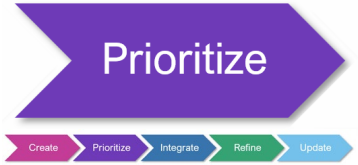
Where to Start?







How to Rollout to Suppliers?



Categorize and Prioritize Components

Hardware

- Active vs passive
- Debug access

Firmware

- Mutable vs immutable
- Firmware storage

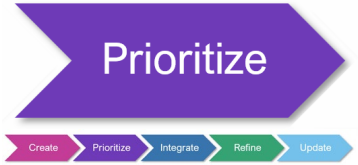
Software

- Runtime environment
- Privileges

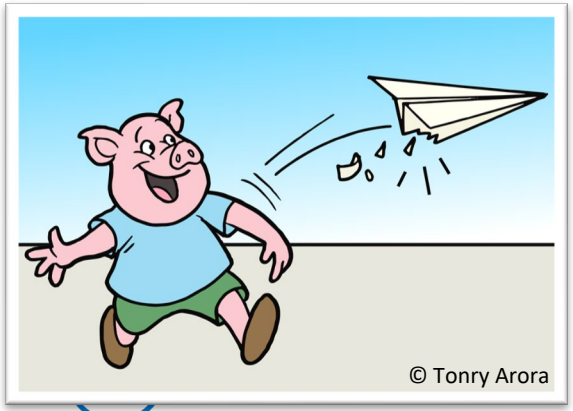
- Function
- Interfaces
- Security requirements
- Threat boundary
- Leveraged
- Number of sources
- Reputation
- SDL maturity (if known)

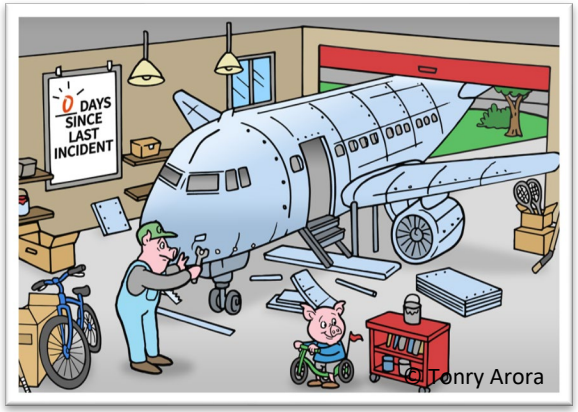
Risk of exploitation and level of impact to customers
Security and business impact

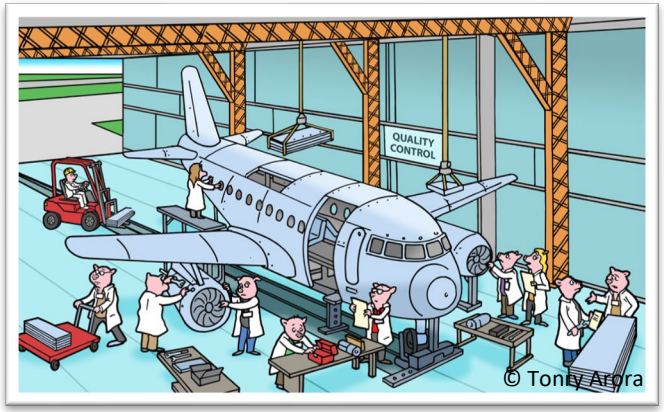
Supplier vs Component Risk

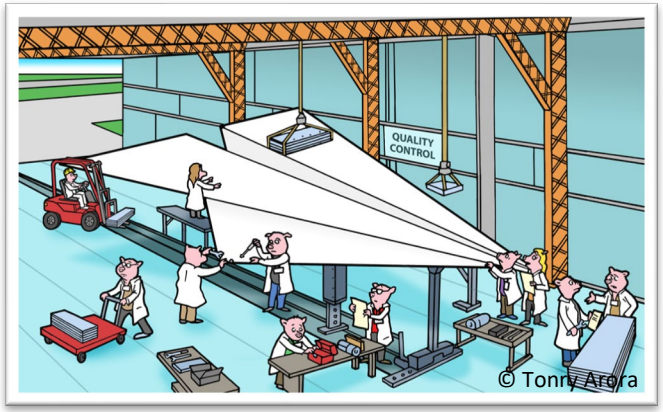


Supplier Risk	Component Risk
High Risk Supplier Low Risk Component(s)	High Risk Supplier High Risk Component(s)
Low Risk Supplier Low Risk Component(s)	Low Risk Supplier High Risk Component(s)

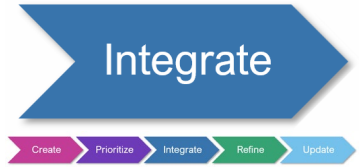






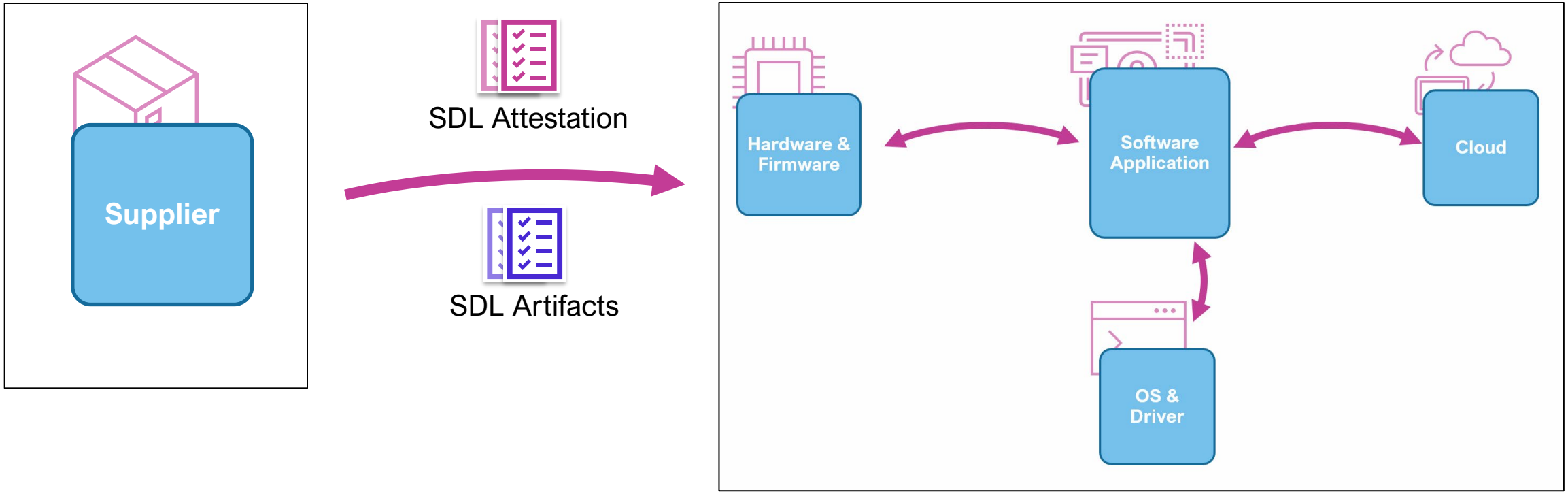


Integrate into Internal Process

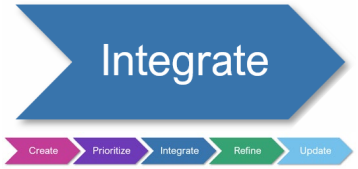


Supplier SDL

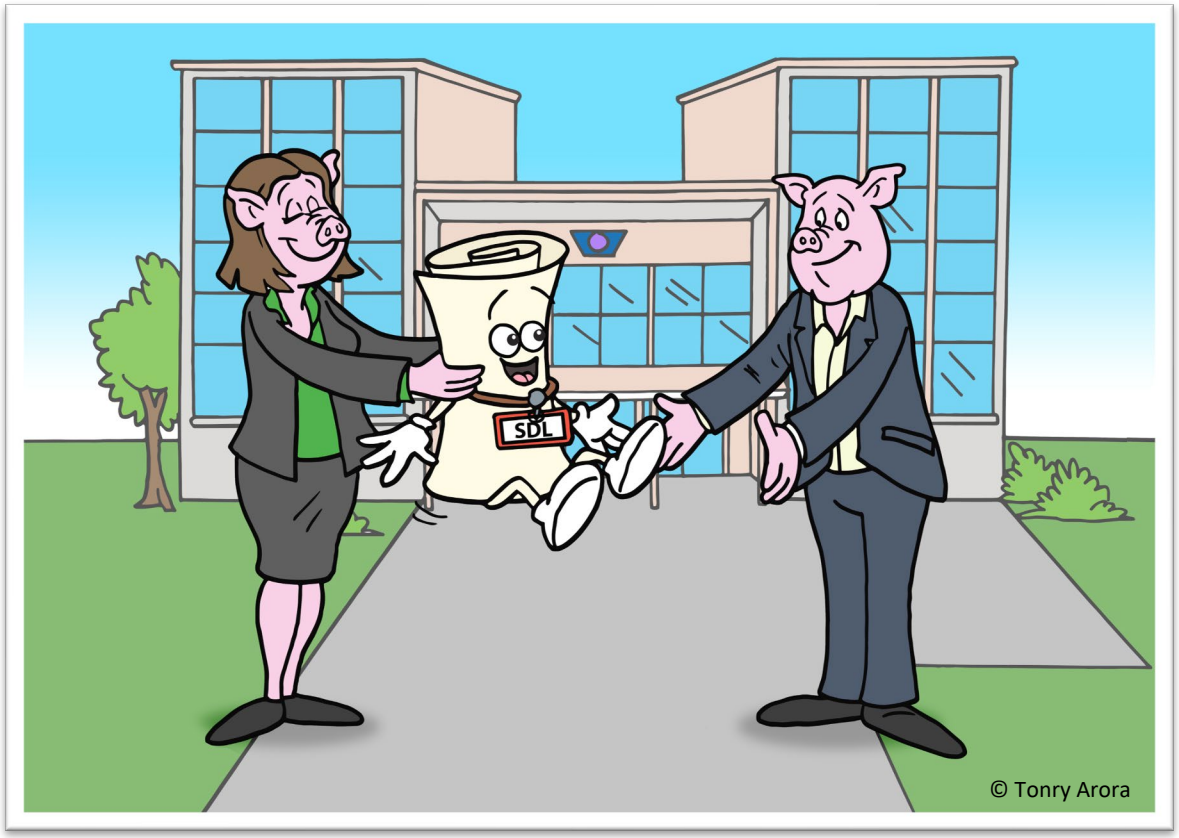
Internal SDL



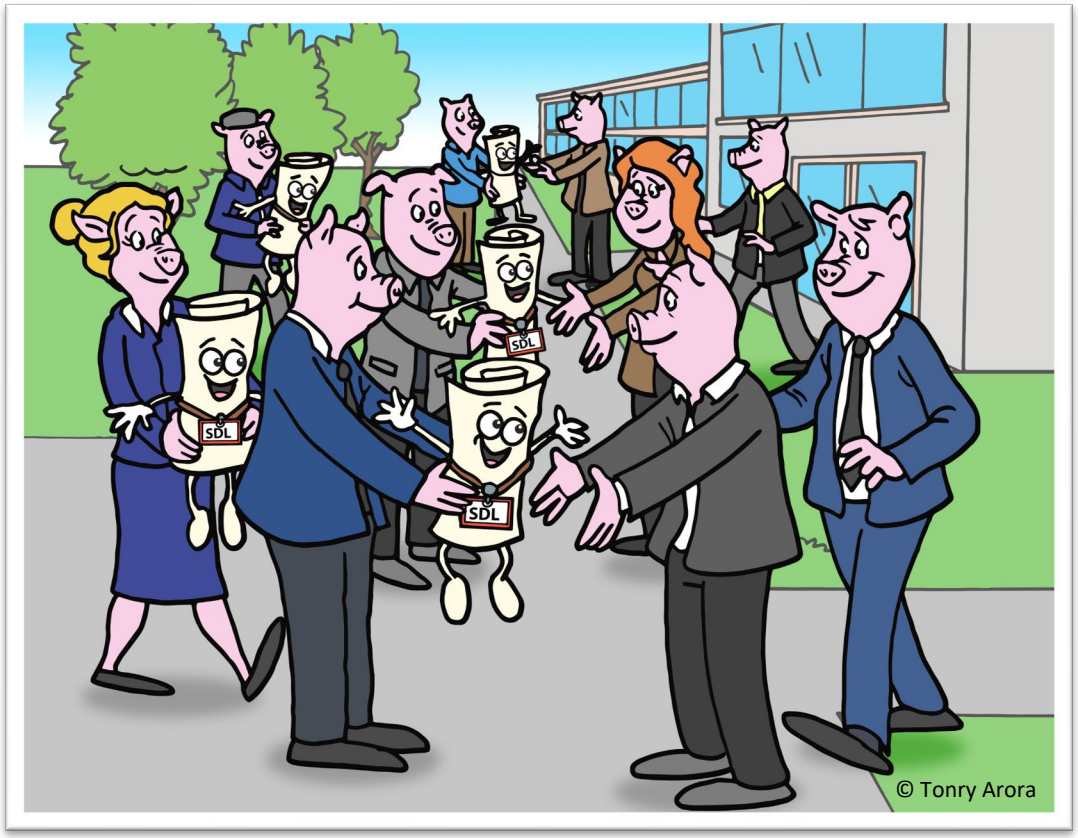
Integrate into Internal Process



Share Artifacts

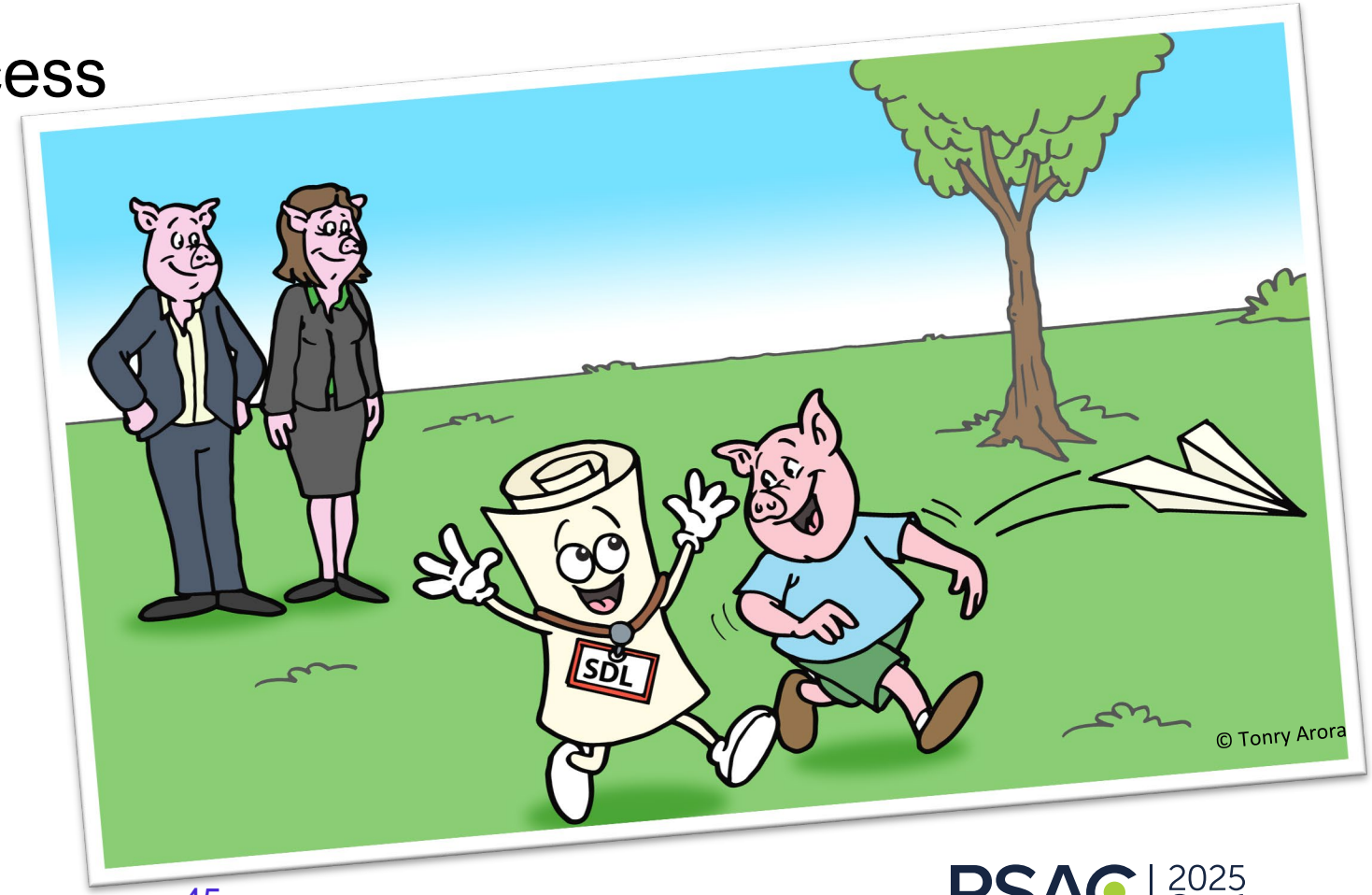


Sharing is Caring



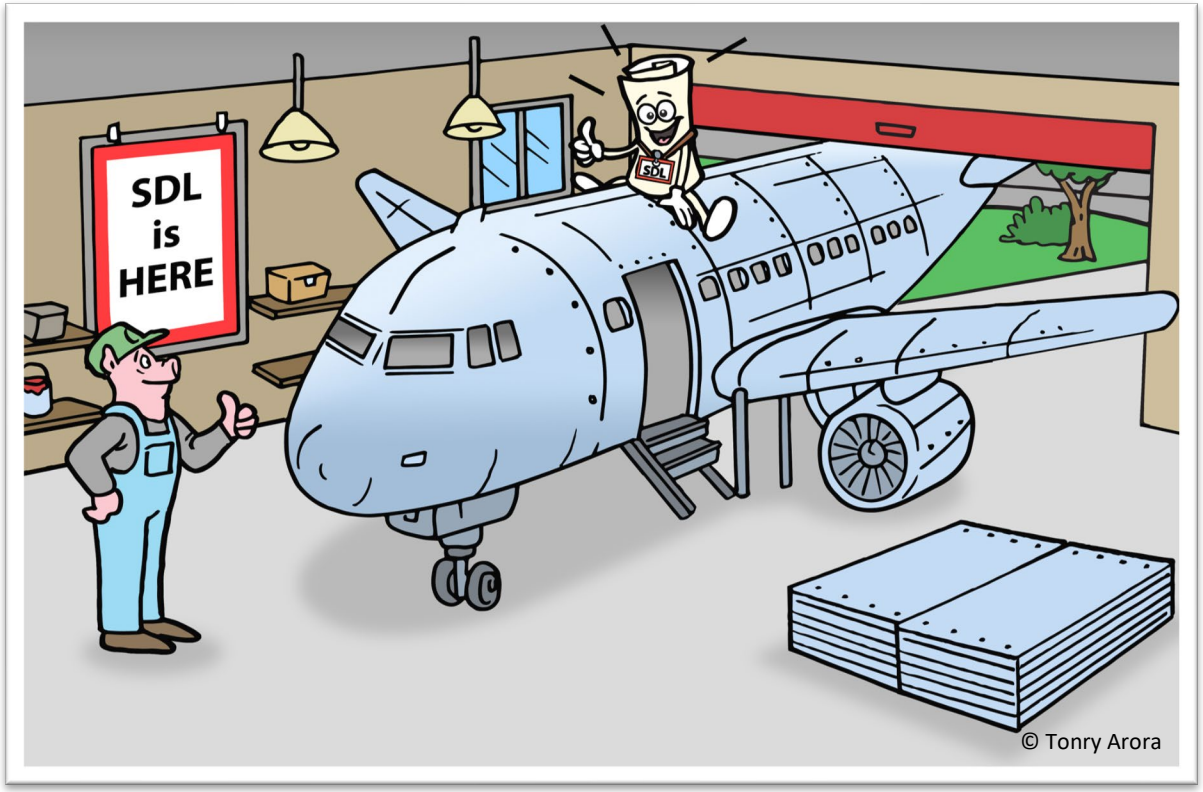
Other Considerations

- Periodic risk review
- Implement exception process
- Automation to scale



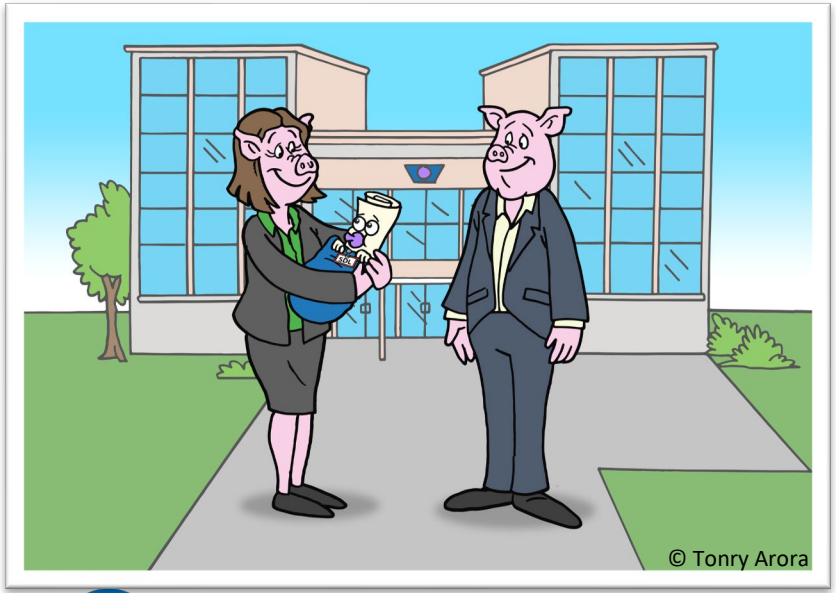
Key Takeaways

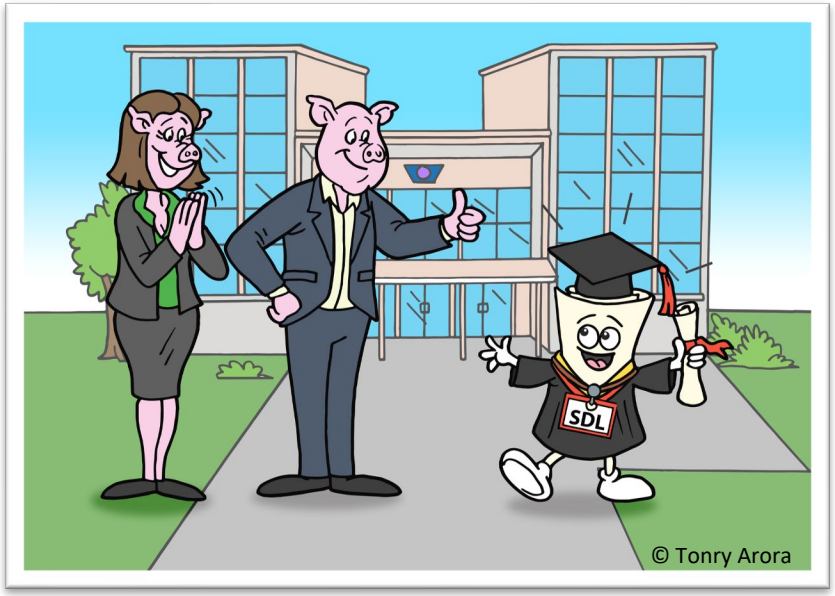
- Shift SDL left
- Risk based approach
- Takes time, but need to start now



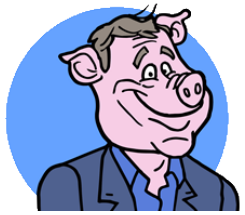
Apply to Your Organization

- Step 1: Define supplier SDL requirements
- Step 2: Rollout SDL requirements
- Step 3: Integration of Requirements, Attestation, and Artifacts





Questions?



Richard Tonry
Distinguished Engineer
Firmware Security Architect
Dell
Richard.Tonry@Dell.com
linkedin.com/in/RichardTonry

Mohit Arora
Senior Distinguished Engineer
Software Security Architect
Dell
Mohit.A@Dell.com
linkedin.com/in/getmohitarora